

# CRL & OCSP report for (ANF Autoridad de Certificacion)



Certificate details CRL Checks OCSP Checks

Error Warning Success Info

Raw data Refresh

- ANF Global Subordinate EV CA1
- ANF Global Root CA

## ["ANF Autoridad de Certificacion"]

Certificate details for certificate with serial number 996319061734379174

(At position 1 in certificate chain)

<b>Serial number:</b> hex: dd3a2e86da0cea6 int: 996319061734379174	<b>Company registration number:</b> G63287510
<b>Issued by:</b> ANF Global Subordinate EV CA1	<b>Organization:</b> ANF Autoridad de Certificacion
<b>Public Key Algorithm:</b> RSA	<b>Organization unit:</b> Certificado Cualificado de Servidor Seguro SSL EV
<b>Not valid before:</b> Oct 1, 2019 12:00:26 PM	<b>State / Province:</b> Barcelona
<b>Not valid after:</b> Sep 30, 2021 12:00:26 PM	<b>Locality:</b> Barcelona
	<b>Country:</b> ES

- ✓ This certificate does not contain any links to an LDAP server
- ✓ This certificate does not contain any internal server links
- ✓ This certificate does not contain any links with an unknown format

Check certificate compliance for

## Certificate Revocation List (CRL)

This CRL was cached at Oct 7, 2019 8:57:21 PM

<http://www.anf.es/crl/ANFGlobalSubordinateEVCA1.crl>

### CRL information

**Source:** CRL Distribution Point listed in Certificate  
**Location:** <http://www.anf.es/crl/ANFGlobalSubordinateEVCA1.crl>  
**Size:** 929 bytes (DER data)  
**Response time:** 316.109023ms  
**This update:** Oct 5, 2019 2:00:18 PM  
**Next update:** Oct 12, 2019 2:00:18 PM  
**Revoked:** No  
**Revoked certificates in CRL:** 2

### Relevant server response headers

**Date:** Oct 7, 2019 8:57:21 PM  
**Last Modified:** Oct 5, 2019 2:00:18 PM  
**Expires:** Oct 12, 2019 2:00:18 PM

### Server and network information

**Server Software:** Apache

- ✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
- ✓ This CRL file is DER encoded
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ ThisUpdate is less than seven days old, CRLs must be updated and reissued at least every seven days (Mozilla Maintenance Policy section 3)
- ✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This CRL was cached at Oct 7, 2019 8:57:21 PM

<http://crl.anf.es/crl/ANFGlobalSubordinateEVCA1.crl>

### CRL information

**Source:** CRL Distribution Point listed in Certificate  
**Location:** <http://crl.anf.es/crl/ANFGlobalSubordinateEVCA1.crl>  
**Size:** 929 bytes (DER data)  
**Response time:** 466.440201ms  
**This update:** Oct 5, 2019 2:00:18 PM  
**Next update:** Oct 12, 2019 2:00:18 PM  
**Revoked:** No  
**Revoked certificates in CRL:** 2

### Relevant server response headers

**Date:** Oct 7, 2019 8:57:21 PM  
**Last Modified:** Oct 5, 2019 2:00:18 PM  
**Expires:** Oct 12, 2019 2:00:18 PM

### Server and network information

**Server Software:** Apache

- ✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)' [↗](#)
- ✓ This CRL file is DER encoded
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ ThisUpdate is less than seven days old, CRLs must be updated and reissued at least every seven days (Mozilla Maintenance Policy section 3) [↗](#)
- ✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements) [↗](#)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) [↗](#)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) [↗](#)

## Online Certificate Status Protocol (OCSP)

This OCSP response was cached at Oct 7, 2019 8:57:21 PM

<http://ocsp.anf.es/spain/AV> (GET)

### OCSP response information

**Source:** OCSP server listed in Certificate  
**Location:** http://ocsp.anf.es/spain/AV  
**Size:** 2481 bytes (DER)  
**Response time:** 317.48143ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** ANF Global Subordinate EV CA1 Responder 1295  
**Issued by:** ANF Global Subordinate EV CA1  
**Signing certificate validity:** Sep 5, 2019 5:04:25 PM - Jul 1, 2020 5:04:25 PM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** Oct 7, 2019 8:57:21 PM  
**Next update:** Oct 14, 2019 8:57:21 PM  
**Produced at:** Oct 7, 2019 8:57:21 PM  
**Server status:** Success  
**Status:** Good

### Relevant server response headers

**Date:** Oct 7, 2019 8:57:21 PM  
**Last Modified:** Oct 7, 2019 8:57:21 PM  
**Expires:** Oct 14, 2019 8:57:21 PM

- ✓ OCSP requests is smaller than 255 bytes [↗](#)
- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ ThisUpdate is less than four days old, OCSP information must be updated at least every four days (Mozilla & Baseline Requirements) [↗](#)
- ✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements) [↗](#)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) [↗](#)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) [↗](#)

This OCSP response was cached at Oct 7, 2019 8:57:21 PM

<http://ocsp.anf.es/spain/AV> (POST)

### OCSP response information

**Source:** OCSP server listed in Certificate  
**Location:** http://ocsp.anf.es/spain/AV  
**Size:** 2481 bytes (DER)  
**Response time:** 322.281151ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** ANF Global Subordinate EV CA1 Responder 1295  
**Issued by:** ANF Global Subordinate EV CA1  
**Signing certificate validity:** Sep 5, 2019 5:04:25 PM - Jul 1, 2020 5:04:25 PM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** Oct 7, 2019 8:57:21 PM  
**Next update:** Oct 14, 2019 8:57:21 PM  
**Produced at:** Oct 7, 2019 8:57:21 PM  
**Server status:** Success  
**Status:** Good

### Relevant server response headers

**Date:** Oct 7, 2019 8:57:21 PM  
**Last Modified:** Oct 7, 2019 8:57:21 PM  
**Expires:** Oct 14, 2019 8:57:21 PM

- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'
- ✓ Response is already valid

- ✓ response is not expired
- ✓ ThisUpdate is less than four days old, OCSP information must be updated at least every four days (Mozilla & Baseline Requirements) [↗](#)
- ✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements) [↗](#)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) [↗](#)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) [↗](#)

This OCSP response was cached at Oct 7, 2019 8:57:21 PM

<http://ocsp.anf.es/spain/AV> (UNKNOWN)

#### OCSP response information

**Source:** OCSP server listed in Certificate  
**Location:** <http://ocsp.anf.es/spain/AV>  
**Size:** 2489 bytes (DER)  
**Response time:** 337.060419ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** ANF Global Subordinate EV CA1 Responder 1295  
**Issued by:** ANF Global Subordinate EV CA1  
**Signing certificate validity:** Sep 5, 2019 5:04:25 PM - Jul 1, 2020 5:04:25 PM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** Oct 7, 2019 8:57:21 PM  
**Next update:** Oct 14, 2019 8:57:21 PM  
**Produced at:** Oct 7, 2019 8:57:21 PM  
**Server status:** Success  
**Status:** Unknown

- ✓ OCSP requests is smaller than 255 bytes [↗](#)
- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'

## ANF Global Subordinate EV CA1 (CA Certificate)

• Certificate details for ANF Global Subordinate EV CA1

(At position 2 in certificate chain)

<b>Serial number:</b> hex: 162091c6629b423 int: 99652159333315619 <b>Issued by:</b> ANF Global Root CA <b>Public Key Algorithm:</b> RSA <b>Not valid before:</b> Sep 5, 2019 5:00:39 PM <b>Not valid after:</b> Sep 2, 2029 5:00:39 PM	<b>Company registration number:</b> G63287510 <b>Organization:</b> ANF Autoridad de Certificacion <b>Organization unit:</b> ANF Autoridad intermedia tecnicos <b>Country:</b> ES
--	---

- ✓ This certificate does not contain any links to an LDAP server
- ✓ This certificate does not contain any internal server links
- ✓ This certificate does not contain any links with an unknown format

[Check certificate compliance for ANF Global Subordinate EV CA1](#)

## Certificate Revocation List (CRL)

This CRL was cached at Oct 3, 2019 12:19:40 PM

[http://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_ari.crl](http://crl.anf.es/crl/ANF_Global_Root_CA_2036_ari.crl)

#### CRL information

**Source:** CRL Distribution Point listed in Certificate  
**Location:** [http://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_ari.crl](http://crl.anf.es/crl/ANF_Global_Root_CA_2036_ari.crl)  
**Size:** 846 bytes (DER data)  
**Response time:** 461.999198ms  
**This update:** Jun 7, 2019 6:47:47 PM  
**Next update:** Dec 4, 2019 6:47:47 PM  
**Revoked:** No  
**Revoked certificates in CRL:** 0

#### Relevant server response headers

**Date:** Oct 3, 2019 12:19:40 PM  
**Last Modified:** Jun 7, 2019 6:47:47 PM  
**Expires:** Dec 4, 2019 6:47:47 PM

#### Server and network information

**Server Software:** Apache

- ✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)' [↗](#)
- ✓ This CRL file is DER encoded
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ Revocation information is updated at least once every twelve months [↗](#)
- ✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field [↗](#)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) [↗](#)

- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) [↗](#)

This CRL was cached at Oct 3, 2019 12:19:40 PM

[http://www.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_ari.crl](http://www.anf.es/crl/ANF_Global_Root_CA_2036_ari.crl)

#### CRL information

**Source:** CRL Distribution Point listed in Certificate  
**Location:** [http://www.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_ari.crl](http://www.anf.es/crl/ANF_Global_Root_CA_2036_ari.crl)  
**Size:** 846 bytes (DER data)  
**Response time:** 296.974098ms  
**This update:** Jun 7, 2019 6:47:47 PM  
**Next update:** Dec 4, 2019 6:47:47 PM  
**Revoked:** No  
**Revoked certificates in CRL:** 0

#### Relevant server response headers

**Date:** Oct 3, 2019 12:19:40 PM  
**Last Modified:** Jun 7, 2019 6:47:47 PM  
**Expires:** Dec 4, 2019 6:47:47 PM

#### Server and network information

**Server Software:** Apache

- ✓ Content-Type in response is set to 'application/pkix-crl' (RFC 5280, section 4.2.1.13) [↗](#)
- ✓ This CRL file is DER encoded
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ Revocation information is updated at least once every twelve months [↗](#)
- ✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field [↗](#)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) [↗](#)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) [↗](#)

## Online Certificate Status Protocol (OCSP)

This OCSP response was cached at Oct 3, 2019 12:19:40 PM

<http://ocsp.anf.es/spain/AV> (GET)

#### OCSP response information

**Source:** OCSP server listed in Certificate  
**Location:** <http://ocsp.anf.es/spain/AV>  
**Size:** 2559 bytes (DER)  
**Response time:** 322.329895ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** ANF Global Root CA 2036 Responder 1273  
**Issued by:** ANF Global Root CA  
**Signing certificate validity:** Jul 9, 2019 5:02:29 PM - May 4, 2020 5:02:29 PM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** Oct 3, 2019 12:19:40 PM  
**Next update:** Oct 10, 2019 12:19:40 PM  
**Produced at:** Oct 3, 2019 12:19:40 PM  
**Server status:** Success  
**Status:** Good

#### Relevant server response headers

**Date:** Oct 3, 2019 12:19:40 PM  
**Last Modified:** Oct 3, 2019 12:19:40 PM  
**Expires:** Oct 10, 2019 12:19:40 PM

- ✓ OCSP requests is smaller than 255 bytes [↗](#)
- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ Revocation information is updated at least once every twelve months [↗](#)
- ✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field [↗](#)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) [↗](#)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) [↗](#)

This OCSP response was cached at Oct 3, 2019 12:19:40 PM

<http://ocsp.anf.es/spain/AV> (POST)

#### OCSP response information

**Source:** OCSF server listed in Certificate  
**Location:** http://ocsp.anf.es/spain/AV  
**Size:** 2559 bytes (DER)  
**Response time:** 321.31979ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** ANF Global Root CA 2036 Responder 1273  
**Issued by:** ANF Global Root CA  
**Signing certificate validity:** Jul 9, 2019 5:02:29 PM - May 4, 2020 5:02:29 PM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** Oct 3, 2019 12:19:40 PM  
**Next update:** Oct 10, 2019 12:19:40 PM  
**Produced at:** Oct 3, 2019 12:19:40 PM  
**Server status:** Success  
**Status:** Good

#### Relevant server response headers

**Date:** Oct 3, 2019 12:19:40 PM  
**Last Modified:** Oct 3, 2019 12:19:40 PM  
**Expires:** Oct 10, 2019 12:19:40 PM

- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ Revocation information is updated at least once every twelve months
- ✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This OCSP response was cached at Oct 3, 2019 12:19:40 PM

http://ocsp.anf.es/spain/AV (UNKNOWN)

#### OCSP response information

**Source:** OCSF server listed in Certificate  
**Location:** http://ocsp.anf.es/spain/AV  
**Size:** 2567 bytes (DER)  
**Response time:** 341.909279ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** ANF Global Root CA 2036 Responder 1273  
**Issued by:** ANF Global Root CA  
**Signing certificate validity:** Jul 9, 2019 5:02:29 PM - May 4, 2020 5:02:29 PM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** Oct 3, 2019 12:19:40 PM  
**Next update:** Oct 10, 2019 12:19:40 PM  
**Produced at:** Oct 3, 2019 12:19:40 PM  
**Server status:** Success  
**Status:** Unknown

- ✓ OCSP requests is smaller than 255 bytes
- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'

## ANF Global Root CA (CA Certificate)

Certificate details for ANF Global Root CA

(At position 3 in certificate chain)

**Serial number:**  
**hex:** 16495ee618a0750  
**int:** 100369942780184400  
**Issued by:** ANF Global Root CA  
**Public Key Algorithm:** RSA  
**Not valid before:** May 20, 2016 4:08:40 PM  
**Not valid after:** May 15, 2036 4:08:40 PM

**Company registration number:** G63287510  
**Organization:** ANF Autoridad de Certificacion  
**Organization unit:** ANF Clase 1 CA  
**Country:** ES

- ✓ This certificate does not contain any links to an LDAP server
- ✓ This certificate does not contain any internal server links
- ✓ This certificate does not contain any links with an unknown format

This is a self signed certificate

[Check certificate compliance for ANF Global Root CA](#)

[Check the revocation status for another website](#)

## Check the revocation status for another website

Created by Paul van Brouwershaven

◆ 2015 - 2019 Digitorus B.V.

*Revoked certificates can't and should not be trusted, these certificate will cause errors like "NET::ERR\_CERT\_REVOKED" in browsers and expose a security risk.*